Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

The Information Commissioner's response to a call for evidence on digital identity from the Secretary of State for the Department for Digital, Culture, Media and Sport

1. The Information Commissioner has responsibility for promoting and enforcing the EU General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA18), the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR); the Privacy and Electronic Communications Regulations 2003 (PECR); the INSPIRE Regulations; eIDAS Regulations; Re-use of Public Sector Information Regulations; and the NIS Regulations.

2. The Information Commissioner is independent of government and upholds information rights in the public interest, promoting transparency and accountability by public bodies and organisations and protecting individuals' privacy and information access rights.

3. The Information Commissioner's Office (ICO) welcomes the opportunity to respond to the government's call for evidence on supporting improvements in identity verification and the development and secure use of digital identities.

Introduction

4. People want to be able to identify themselves easily and securely when accessing digital services and have control and choice over the use of their data wherever possible. The providers of digital services and products also want to have a reliable way to ensure they are dealing with the right people and can rely on the attributes being asserted.

5. The call for evidence rightly identifies the importance of an effective and secure digital identity system or infrastructure in supporting innovation, reducing fraud and costs, and safeguarding privacy. The Information Commissioner has made clear her commitment to privacy and innovation working hand in hand in today's evolving digital economy. It is essential that the government builds privacy and data protection into the development of public policy on digital identity.

6. Effective, modern data protection laws with robust safeguards have a central part to play in securing the public's confidence in the use of their personal information within the digital economy and the delivery of public and private services and products. Improvements to identity verification can only be fully realised and opportunities maximised if risks around privacy and data processing are adequately addressed.

7. This response covers the four main topics identified in the call for evidence, with a focus on providing relevant evidence from a privacy perspective. A number of key concepts and principles run through our response including: trust; transparency; accountability; privacy by design; security and data minimisation. It is essential that these principles and concepts should be at the heart of any new digital identity system.

Needs and problems

Addressing questions 1,2,3,4,5,6

8. As outlined in the call for evidence, proving identity online can sometimes be difficult for both individuals and organisations. It is important that people are able to prove who they are in a secure and reliable way or to prove that they have a particular attribute. Any digital identity solution needs to find a balance between verifying the identity or attributes of an individual and minimising the collection and retention of personal data.

9. Problems arise when people are asked to provide far more personal information than is necessary. This not only increases information risk but can result in a lack of public trust, for example if there is function creep and excessive data is collected for identification but is seen as valuable for marketing. There are also risks if multiple organisations hold duplicate data that could be hacked or misused. We are keen to avoid a situation where organisations build intrusive, granular databases and are then able to track how people live their lives.

10. Individuals must have confidence that their personal data will be handled responsibly in any new digital identity system. We want to promote privacy friendly solutions. At its simplest any digital identity infrastructure should serve to minimise risk by not collecting unnecessary data; avoiding central collections of data; generating persistent records of where identity is asserted in different contexts; preventing the replication of data in multiple locations; and not requiring the transmission of detailed information rather than verifying facts.

11. If a new identity system embraces the need for 'baked in' privacy safeguards from first principles it should reduce risk. A privacy friendly, data protection compliant, identity infrastructure can then realise many benefits and opportunities – from economic growth and technological innovation to the delivery of more efficient and tailored public services, including other benefits for individuals such as not excluding those who may find it hard to assert their identity and attributes through existing means.

12. Individuals are often legally required to provide data to government bodies. Given that they have no choice and these obligations are focussed

on achieving the limited pressing needs that justify statutory compulsion, we would expect this data to be treated with extra care and be protected by compensatory safeguards against unwarranted wider use.

Learning lessons

13. Developing reliable and trustworthy solutions to establish digital identity is not easy. The ICO has worked with the Privacy and Advisory Consumer Group (PCAG) in an advisory capacity. We would encourage the government to learn lessons from Verify given the investment and useful work on developing privacy friendly approaches, as well as from some of the difficulties the programme has faced. The NAO in its investigation into Verify[1] outlined some of the challenges including maintaining a clear strategic direction; falling short of achieving over-ambitious targets on scale, timing and costs and achieving buy-in from other government departments.

14. The NAO report also highlights GDS's achievements in strengthening online identity while maintaining a high degree of privacy through helping define standards; building the platform and developing the market of private sector identity providers. The ICO supported features such as the establishment of PCAG; the development of open standards; and building in privacy using a federated approach rather than developing a central database. We recommend the government builds on this work.

Trust

15. People want secure and convenient access to products and services and an effective way of identifying themselves, but they also want to know how and why their data will be used. They want their privacy to be respected, so if their data is processed or shared, they can be assured that it will be used reliably, in ways they understand and expect and kept securely. If organisations can show them that their data is used responsibly, people are more likely to trust them with their data.

16. The accountability and fairness principles in GDPR and DPA 2018 place a responsibility on organisations, including government, to understand the risks they create for others with their data processing, and to mitigate those risks before they manifest themselves. Data protection needs to be part of the cultural and business fabric of any organisation processing personal data for digital identity purposes.

Safeguards

17. We recognise there can be benefits in the government developing a digital identity system where trusted identities can be used in more than one

[1] https://www.nao.org.uk/report/investigation-into-verify/

place but such a system must inspire confidence. Data protection safeguards have a central part to play, including those below.

Data minimisation

18. Data minimisation is a core requirement of data protection legislation. Acquiring, using and retaining the minimum amount of data necessary reduces privacy risks. Organisations must comply with the minimisation principle which means ensuring that any personal data is adequate, relevant and limited to what is necessary for the purposes for which it is processed.

Accountability:

19. Accountability enables organisations to show and prove how they respect people's privacy rights, which helps to develop and sustain people's trust. It is no longer sufficient just to comply with the law. Organisations need to actively demonstrate their compliance by embedding privacy principles into their systems and processes and manage risk.

20. We recommend the development of new identity solutions recognises the importance of meeting the requirements of the accountability principle as part of participating organisations' compliance with data protection legislation. Accountability requires organisations to be on the front foot demonstrating their organisational commitment and privacy safeguards. There are a variety of key aspects to consider including:

Data protection by design and default:

21. Data protection by design and default is about considering data protection and privacy issues at the outset. It can help organisations ensure that they comply with the GDPR's fundamental principles and requirements.

22. Organisations should build in data protection requirements from the outset, not bolted on to an existing systems. DPIAs have a crucial role to play in a virtuous lifespan of privacy controls from planning to delivery and operation. Privacy-enhancing technologies or PETs are technologies that embody fundamental data protection principles by minimising personal data use, maximising data security, and empowering individuals.

23. Any identity system should have robust governance arrangements in place and be clear on responsibilities, liabilities and redress. These are important not just for compliance but setting a strong culture.

Codes of conduct and certification:

24. These are regulatory mechanisms that provide opportunities for organisations to adhere to a common set of more particular standards in

the form of a code of conduct and the ability to gain and maintain independent certification of their adherence to these standards. This approach may have significance to the management of a digital identity infrastructure across a wide number of participants.

Data quality and security

25. There should be robust arrangements in place to ensure the quality of the underlying data in any digital identity solution in terms of accuracy, being up to date and being relevant. Incorrect or out of date information could lead to individuals being unfairly refused services. Any identity solution should be based on strong technical and organisational security arrangements, including the use of privacy-enhancing technologies, in order to minimise the risk of fraud, impersonisation and other misuse or loss of data. Systems should be kept under regular review, monitoring false positive rates etc.

Individual rights

26. A digital identity infrastructure should be designed to facilitate the exercise of individuals' rights under the DPA, for example ease of access to data without forcing individuals to use statutory backstop rights to access their information. Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR and helps organisations build a trustworthy reputation.

Criteria for trust (*Addressing questions 7, 8. 9)*

27. Drawing on our experience of regulating eIDAS and advising on identity issues, we recommend that any digital identity scheme should be transparent, open and focussed on the citizen user. Public trust will be gained through the adoption of solutions that put users and their privacy at the heart of these. This enables organisations to establish and demonstrate their commitment to user privacy whilst providing users with control over the use of their data through data minimisation techniques and privacy enhancing technologies. Solutions must incorporate strong privacy engineering and incorporate the principles of privacy and data protection by design and default in accordance with GPDR.

28. Alignment or interoperation with EU and international standards will be required to support cross-border user identification as required e.g. eIDAS for eID interoperability and Trust Services standards to ensure common assurance for organisations supporting identity initiatives.

29. We recommend a federated strategy to distribute the use and collection of personal data and decouple identity management from relying party

services. Also an identity architecture framework and components for participant re-use and development. The building blocks could include:

- technical specifications and standards;
- compliant sample software for re-use (for integration with relying party applications, interoperability purposes etc);
- support services, for example conformance testing, help and advice, to support the developing community.

30. A new identity scheme will require a policy and legal framework incorporating agreed identity management, privacy principles and roles, responsibilities, liabilities etc of all participants. This is necessary to ensure risks are distributed and mitigated as required; appropriate privacy and data protection controls are in place; and to establish and demonstrate scheme trust and integrity for all parties.

Assurance and certification

31. Digital identity schemes should be built to common and open standards, aligned to EU and other international standards as required e.g. for identity proofing - eIDAS assurance levels, UK GPGxx standards, BSI 29003:2018, NIST 800-63 etc. For technical interoperability with EU, adoption of the eIDAS interoperability framework.

32. Common assurance standards across the framework should build public trust so long as they are understandable and consistent. Certification similarly should allow the user to be assured they are using a protected and private service.

33. A failure to ensure appropriate assurance standards is likely to result in a lack of public trust leading to significant issues in on boarding new users. Without common standards the ubiquity and therefore overall value of the service will decrease, limiting further investment.

Approach that protects privacy of users, covers a range of technologies and responds appropriately to innovation (such as biometrics)

34. We recommend that any digital identity scheme should be built upon a set of foundation principles or standards which accommodate change and innovation and are agreed by stakeholders and participant representatives. Existing examples of these that go beyond compliance with DP law that should be consulted and reviewed for consideration are:

    - Cabinet Office and GDS guidelines on identity proofing and credentials[2]

[2] https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

- Identity Management and Privacy Principles (Scottish Government, 2014)
- Privacy and Consumer Advisory Group Identity Assurance Principles[3]
- ENISA – EU Agency for Cybersecurity.

35. Standards should be subject to regular review by an appropriate steering committee or oversight body built in the concept of the digital identity framework. Without pre-established review points a digital identity framework is likely to fall behind pace of change. The use of new technologies should be assessed against privacy impacts and should be commensurate with the aims likely to be achieved in their implementation. Particular attention should be paid to the concept of template ownership and appropriate controls and security provisions.

Biometric data

36. Under data protection law, biometrics are special category data and will require considerations of necessity and proportionality which should cover the adequacy and accuracy of the system and any potential risk of harm to individuals. This can include discriminatory impacts regarding protected characteristics, for example, facial recognition technology (FRT) and race or religious clothing. Any providers of such services will be required to support a controller in the production of their DPIA, and will have to provide specific assurances that appropriate safeguards including security provisions are in place.

37. Any proposed use of biometric data will require a DPIA where that processing is large scale or involves data matching. It is likely that most forms of digital identity services envisaged by the call for evidence will require this. More information can be found in our DPIA guidance on our list of processing activities likely to result in high risk – federated identity assurance services is one example we cite[4].

38. As part of this impact assessment, organisations will have to describe their intended processing and its scope, as well as consider the legal framework. This helps address these matters at the outset, building in and not bolting on safeguards as a necessary but expensive afterthought.

[3] https://www.gov.uk/government/publications/govuk-verify-identity-assurance-principles/identity-assurance-principles

[4] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/)

Human Rights Act

39. Under data protection law, any processing must be fair and lawful. Organisations must ensure that they do not breach other laws, including on human rights. Processing has to be compliant with Article 8 of the Human Rights Act and necessary, proportionate and for a pressing social need for it to be lawful. A DPIA should include and address these wider legal considerations.

40. Biometrics are special category data and will require considerations of necessity and proportionality which can include discriminatory impacts. Any providers of services will be required to support a controller in the production of their DPIA, and provide assurances that appropriate safeguards are in place.

Role of government

41. Often individuals are required to provide their data to government bodies under statute or other obligations. This statutory compulsion gives them no discretion on whether to provide the details or choose on how these are used. Personal data obtained in this way needs to be treated with extra care and protected by compensatory safeguards to ensure that subsequent use is not incompatible with the reason why statutory compulsion was required. There cannot be compulsion to provide personal data to deliver an important public service and then use this for services that would not justify such an obligation without recourse back to the individual or specific legal provision.

42. Government may need to provide more help for individuals with "thin files", some of whom may be vulnerable, to use digital identity services. There may be a need for a public sector ID provider.

43. We welcome the proposal to use small-scale pilots initially to allow organisations to check people's identity using British passport data where they use this to register for government services but care needs to be taken to ensure this does not result in adverse privacy consequences. We will follow the progress of the pilots with interest. Evaluation of the pilots should include privacy issues and other requirements such as security, data quality, governance arrangements and clear responsibilities.

Legislation and statutory regulation

44. Data protection law requires public authorities to have a lawful basis for processing data. We recognise that specific legislation for a digital identity framework could provide a clear basis for processing personal data and bring clarity on safeguards. We would strongly favour a permissive legislative regime rather than one based on legal obligations.

45. It is important that specific legislation for a digital identity system must be consistent with the requirements of data protection legislation. Any codes or guidance should be closely aligned with those produced by the ICO, for example on transparency; principles such as minimisation and data quality; security; and data protection impact assessments. This will help practitioners gain a clearer understanding of the whole legislative framework and lead to greater harmonisation and consistency between the legal provisions. It will also help put the protection of privacy at the centre of any government digital identity initiative.

Role of the private sector

46. We understand and support the potential benefits of improved digital identity requirements for both public and private sectors but these developments must proceed in accordance with data protection law and reflect its core principles to inspire public trust and confidence. Data protection can help enable the development of a comprehensive approach to digital identity solutions given its wide-ranging application.

47. Innovation in the digital economy relies on consumers allowing businesses to re-use previously verified identities or attributes provided for other purposes. This is more likely if they have confidence that they can be relied upon to handle their personal data securely and respect their privacy, choices and rights.

48. Re-use of personal data held by the public sector should be based on attribute checking and verifying facts rather than requiring sharing or transmitting detailed personal information provided to the public sector. We would expect the private sector to be fully consulted on standard setting and the design of a comprehensive digital identity infrastructure, drawing on their expertise and experience of their current processes of verifying identity such as know your customer and provision of identity services.

September 2019